



IT Security Handbook

Awareness and Training

ITS-HBK-2810.06-01 -
Effective Date: 20110506 -
Expiration Date: 20130506 -
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.06-01)
Awareness and Training

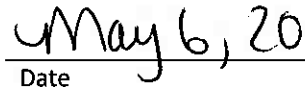
Distribution:

NODIS

Approved



Valarie Burks
Deputy Chief Information Officer for
Information Technology Security



Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Draft

Table of Contents

Change History.....	2 -
1 Introduction and Background.....	4
2 Security Awareness (AT-2)	4
3 Security Training (AT-3)	5
4 Security Training Records (AT-4).....	6
5 Organizationally Defined Values.....	7

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Awareness and Training (AT) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - The Security Awareness and Training control family relates to the information security knowledge requirements for all users of Agency information systems, and the development and delivery of courses and other training resources to enable and validate satisfaction of those requirements. NASA Users are responsible for meeting Agency security training requirements in order to gain and maintain access to any NASA information system resource. Furthermore, certain roles at NASA, including managers and those with significant information security responsibilities, have to comply with additional security training and awareness requirements.
- 1.7 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 1441.1, NASA Records and Retention Schedule*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-2810.15-02, Managed Elevated Privileges*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-16, Information Training Security Requirements; A Role- and Performance-Based Model*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-50, Building an Information Technology Security Awareness and Training Program*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*

2 Security Awareness (AT-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 *The Senior Agency Information Security Officer (SAISO) shall:*
- 2.1.1.1 Ensure the availability of annual security awareness training for the Agency.
- 2.1.2 - *The Center Chief Information Security Officer (CISO) shall: -*

ITS Handbook (ITS-HBK-2810.06-01) -
Awareness and Training -

- 2.1.2.1 Maintain oversight of information security awareness training completion by Center personnel through the System for Administration, Training, and Education Resources for NASA (SATERN).
- 2.1.2.2 Ensure the delivery of training to personnel through alternative means, when necessary.
 - 2.1.2.2.1 Substitution of alternative training for the NASA information security awareness training shall not be allowed unless prior approval has been obtained from the SAISO.
 - 2.1.2.2.2 If an alternate method of training delivery is used, the training Instructor shall provide the Center CISO with:
 - a. A brief summary of the methods of training delivery used;
 - b. A statement that the NASA information security awareness course content was used for the training; and
 - c. A list of trainees with both printed/typed names and signature of the individual that attended the training.
- 2.1.2.3 Ensure the completion of training statistics report actions as assigned by the Office of the Chief Information Officer (OCIO).
- 2.1.3 *The Organization Computer Security Official (OCSO) shall:*
 - 2.1.3.1 Maintain oversight of information security awareness training completion by organizational personnel.
- 2.1.4 *The ISO shall:*
 - 2.1.4.1 Ensure all users with logon access to information systems or applications under their purview complete the information security awareness training prior to authorizing access and annually thereafter as long as access to NASA information, information systems, or IT resources continues.
 - 2.1.4.2 Ensure that user access to NASA information systems or applications under their purview is terminated, including the administrative and/or privileged access, if the required annual or other specified information security-related training is not completed.
- 2.1.5 *The NASA User shall:*
 - 2.1.5.1 Complete the Information Security Awareness training prior to accessing NASA information systems and applications and annually thereafter as long as access to NASA information, information systems, or IT resources continues.
- 2.1.6 *The Information Technology Security Awareness and Training Center (ITSATC) shall:*
 - 2.1.6.1 Author and maintain security awareness training for use across the Agency.
 - 2.1.6.1.1 SATERN shall be used to provide, manage, and record security awareness training.

3 Security Training (AT-3)

3.1 Roles and Responsibilities

- 3.1.1 *The Center CISO shall:*
 - 3.1.1.1 Maintain oversight of the completion of role-based information security training to ensure initial and annual refresher training is completed by Center personnel approved for administrative and/or privileged access to NASA information, information systems and/or IT resources, in accordance with procedures outlines by *ITS-HBK-2810.15-02*.
- 3.1.2 *The OCSO shall:*
 - 3.1.2.1 Maintain oversight of the completion of role-based information security training to ensure initial and annual refresher training is completed by organizational personnel approved for administrative and/or privileged access to NASA information, information systems and/or IT resources, in accordance with procedures outlines by *ITS-HBK-2810.15-02*.
- 3.1.3 *The ISO shall:*

- 3.1.3.1 Ensure roles with significant information security responsibilities or privileged access to NASA information systems are documented in the SSP.
- 3.1.3.2 Ensure the individuals with significant information security responsibilities or privileged access to NASA information systems complete required role-based training and are capable of performing assigned roles and responsibilities.
- 3.1.3.3 Ensure individuals with significant information security responsibilities or privileged access to NASA information systems complete annual refresher training as required.
- 3.1.4 *The NASA User shall:*
 - 3.1.4.1 Complete appropriate role-based information security-related training, as outlined in *ITS-HBK-2810.150-02*, that addresses the procedures and processes necessary to meet the security requirements of the position before being authorized privileged access to the information, information system and/or IT resources and complete the training annually thereafter.
- 3.1.5 *The ITSATC Project Manager shall:*
 - 3.1.5.1 Identify and document those roles that have significant information security responsibilities that require initial and annual role-based information security training in accordance with *NIST SP 800-16, Information Training Security Requirements; A Role- and Performance-Based Model* and *NIST SP 800-50, Building an Information Technology Security Awareness and Training Program*.
 - 3.1.5.1.1 SATERN shall be used to provide, manage, and record role-based information security training.

4 Security Training Records (AT-4)

4.1 Roles and Responsibilities

- 4.1.1 *The SAISO shall:*
 - 4.1.1.1 Ensure completion of Information Security Awareness and role-based information security training is tracked using the SATERN Learning Management System (LMS) and training records destroyed 5-years after separation of employee or when no longer needed in accordance with *NPR 1441.1, NASA Records and Retention Schedule*.
 - 4.1.1.2 Annually review, and update as required, the Security Training Records (AT-4) control requirements as part of the annual assessment of this Agency common control.
- 4.1.2 *The ITSATC Project Manager shall:*
 - 4.1.2.1 Maintain and track all NASA information security awareness training and role-based training documentation and modules for compliance.
 - 4.1.2.2 Utilize SATERN to:
 - 4.1.2.2.1 Assign and monitor progress of Information Security Awareness training compliance.
 - 4.1.2.2.2 Track employee role-based information security training requirements and completion status.
 - 4.1.2.2.3 Serve as the central repository for all NASA information security-related training documentation.

5 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

800 53 Reference							FIPS 199 Categorization		
Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
AT	01	Security Awareness and Training Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
AT	02	Security Awareness	Main	[1]	Frequency	Completion of Basic Security Awareness and Training, following initial training.	1/Year	1/Year	1/Year
AT	03	Security Training	Main	[1]	Frequency	Completion of Role-Based Training for personnel with significant security responsibilities, following initial training.	1/Year	1/Year	1/Year
AT	03	Security Training	E 1	[1]	Frequency	Training for the employment and operation of environmental controls.			
AT	03	Security Training	E 2	[1]	Frequency	Training for the employment and operation of physical controls.			
AT	04	Security Training Records	Main	[1]	Time Period	Individual security training records retention.	As defined by NPR 1441.1	As defined by NPR 1441.1	As defined by NPR 1441.1